CBCS SCHEME

USN | | | | | | | | | | |

15EC744

Seventh Semester B.E. Degree Examination, Jan./Feb. 2023
Cryptography

Time: 3 hrs. Max. Marks: 80

Note: Answer any FIVE full questions, choosing ONE full question from each module.

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.
2. Any revealing of identification, appeal to evaluator and /or equations written eg, 42+8 = 50, will be treated as malpractice.

Module-1

1 a. Write the Euclid's algorithm for determining the GCD of two positive integers. Find the GCD of (1970, 1066) using Euclid's algorithm. **(08 Marks)**

b. Define the following terms with necessary axioms :
(i) Groups (ii) Rings (iii) Fields **(08 Marks)**

OR

2 a. Write the extended Euclid's algorithm for determining the GCD and multiplicative inverse of two integers. Also find the GCD and multiplicative inverse of (4321, 1234). **(08 Marks)**

b. Mention the modular arithmetic properties of congruence with an example. **(06 Marks)**

c. Define relatively prime. Mention an example. **(02 Marks)**

Module-2

3 a. Draw the model of symmetric cryptosystem and explain it. **(08 Marks)**

b. Encrypt the plain text "MONDAY" using Hill Cipher with the key $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$ show your calculation and cipher text. **(08 Marks)**

OR

4 a. Explain with a schematic the classical Fiestel Cipher model. **(08 Marks)**

b. Discuss the concept of play fair cipher algorithm. Using this find the plain text if Cipher text is "OFTIBLDHXM" and key is COMPUTER. **(08 Marks)**

Module-3

5 a. With a neat diagram, explain the various steps involved in AES encryption algorithm. **(08 Marks)**

b. With a neat diagram, explain linear feedback shift Registers. **(08 Marks)**

OR

6 a. With neat block diagram, explain AES key expansion. **(06 Marks)**

b. Write a note on:
(i) Stream Ciphers using LFSR's.
(ii) Design and analysis of Stream Ciphers. **(10 Marks)**

Module-4

7 a. State and prove Fermats theorem. Determine Euler's totient function $\phi(24)$ and $\phi(35)$. **(08 Marks)**

b. In a public key system using RSA, you intercept the Cipher text C = 10 sent to a user whose public key is e = 5, n = 35. What is the plain text M? **(08 Marks)**

OR

8 a. State and prove Chinese remainder theorem. Find x for the following equations:
$X \equiv 2 \bmod 5$, $X \equiv 6 \text{ modulo } 9$ **(05 Marks)**

b. Explain the distribution of secret key using the public key cryptography with confidentiality and authentication. **(05 Marks)**

c. In Diffie Hellman key exchange q = 71, its primitive root α = 7. A′s private key is 5, B′s private key is 12. Find
(i) A′s public key (ii) B′s public key (iii) Shared secret key **(06 Marks)**

Module-5

9 a. Write an explanatory note on message authentication codes. **(08 Marks)**

b. Explain in detail, digital signature algorithm. **(08 Marks)**

OR

10 a. Define one way hash function. Explain the basic uses of hash function with a neat block diagram. **(10 Marks)**

b. Write a note on discrete logarithm signature scheme. **(06 Marks)**

* * * * *

VTU-27-01-2023 01:08:02pm - SN - SN - SN - SN
SN - SN - SN - SN - SN - SN - SN
27-01-2023 01:34:11pm
SN - SN - SN - SN - SN - SN - SN - SN